ADVANCES IN MATHEMATICS 15, 63–92 (1975)

Torsion in Reductive Groups

ROBERT STEINBERG

Department of Mathematics, University of California, Los Angeles, California 90024

INTRODUCTION

In [3, p. E-12], the notion of torsion primes for semisimple algebraic groups was defined (see 2.1 below for a somewhat different definition, for reductive groups), and there it was stated (on p. E-41) without proof that:

0.1 THEOREM. *Let G be a simply connected semisimple algebraic group and t a semisimple element such that $t^n \in Z(G)$, the center of G, for some n divisible by no torsion prime. Then the semisimple component of $Z_G(t)$ is simply connected.*

Our first objective here is to supply a proof of this result and to indicate, as is done in [3], its connection with the problem of extending to several elements the theorem [12, 8.1] that with G as above, $Z_G(t)$ is connected for every semisimple element t. This is done in §2 where various extensions and converses are also considered. This follows preliminary material in §1 where simple proofs of some results of de Siebenthal have been included.

Our second objective is, with the aid of these results, to supply a proof of the following theorem also stated in [3] (on p. E-35).

0.2 THEOREM. *If G is as in* 0.1 *and the characteristic of the base field is not a torsion prime* (*as in* 1.3 *below*), *then $Z_G(H)$ is connected* (*and reductive*) *for every semisimple $H \in \mathfrak{g}$, the Lie algebra of G.*

This and related matters, some also mentioned in [3], are discussed in §3.

Our results were obtained in 1963 at the time of the first writing of [12]. We omitted their proofs from [12] to avoid digressions and from [3] to keep the length down. The starting point, occurring in

607/15/1-5

[12, 1.20], is the theorem that in a finite reflection group acting on real vector space, the centralizer of any collection of points is again a reflection group. In a final section we indicate the extent to which this result holds when the real field is replaced by an arbitrary Abelian group.

The considerations of §2 lead naturally to connections among: the torsion primes, the coefficients of the coroot of the highest root, and the imbeddability of elementary Abelian p-groups in tori. These connections were obtained in [1] for compact Lie groups (which is not an essentially different case), however, with many ad hoc verifications using the classification, as was lamented by Borel himself with the aid of a quotation from G. B. Shaw. For this reason in the present development we have avoided proofs by classification like the plague, even when such proofs could be accomplished "avec un coup d'œuil."

1. The Geometry of the Highest Root

Throughout this work Σ will denote a root system in the classical sense, W its Weyl group, (,) a positive definite inner product invariant under W, $\Sigma^* = \{\alpha^* = 2\alpha/(\alpha, \alpha), \alpha \in \Sigma\}$ the dual system, and V the real space extending $L(\Sigma^*)$, the lattice generated by Σ^*. The elements of Σ should be thought of primarily as functions on L and its extensions such as V. We write $\{\alpha_i, 1 \leqslant i \leqslant r\}$ for a basis (simple system), $-\alpha_0 = \sum_{i=1}^r n_i\alpha_i$ for the corresponding highest root (in case Σ is irreducible), and $-\alpha_0{}^* = \sum n_i{}^*\alpha_i{}^*$ for its coroot. We have

1.1 (a) $n_i{}^* = n_i(\alpha_i, \alpha_i)/(\alpha_0, \alpha_0)$.

(b) If α is a long root (i.e., as long as α_0) and $\alpha^* = \sum m_i{}^*\alpha_i{}^*$, then $m_i{}^* \leqslant n_i{}^*$ for all i.

Here (a) is clear and (b) then follows.

We set $n_0{}^* = 1$ so that

1.2 $$\sum_{i=0}^{r} n_i{}^*\alpha_i{}^* = 0.$$

1.3 Definition. A prime p is a *torsion prime* for a root system Σ if $L(\Sigma^*)/L(\Sigma_1{}^*)$ has p-torsion for some closed subsystem Σ_1 of Σ.

We mean closed with respect to the taking of integral combinations, or, equivalently, negatives and sums, whenever these operations lead to roots. From the definition we get at once:

1.4. If Σ_1 is a closed subsystem of Σ, then the torsion primes for Σ_1 are among those for Σ.

Presently we shall show that p is a torsion prime just when it equals some n_i^* for some irreducible component of Σ.

1.5 LEMMA OF THE STRING. *Let Σ be an irreducible root system and $\alpha_0, \alpha_1, \ldots$ the extended system of simple roots so labeled that $\alpha_0, \alpha_1, \ldots, \alpha_q$ is a minimal string connecting (i.e., $(\alpha_i, \alpha_{i+1}) \neq 0$ for all i) α_0 to a root for which $n^* = \max n_i^*$ is achieved.*

(a) *Each α_i $(0 \leqslant i \leqslant q)$ is a long root and $n_i^* = i + 1$, so that in particular $n^* = q + 1$.*

(b) *If $n^* > 1$, then the string is a simple string connected to the other simple roots only at α_q.*

(c) *If $\{\omega_i \mid 1 \leqslant i \leqslant r\}$ denote the fundamental weights defined by $(\omega_i, \alpha_j^*) = \delta_{ij}$, then for $1 \leqslant i \leqslant q$, ω_i is a sum of long roots, in fact is equal to $-\sum_{j=0}^{i-1} (i - j)\alpha_j$.*

(d) *If v_i in V is defined by $\alpha_j(v_i) = 0$ for $j \neq 0, i$, and $\alpha_0(v_i) = -1$, or, equivalently, $\alpha_i(v_i) = 1/n_i$, then for $1 \leqslant i \leqslant q$ we have $n_i v_i \in L(\Sigma^*)$.*

Proof. If $n^* = 1$, $q = 0$, then the only assertion being made is that α_0 is a long root, which is, of course, well-known (see, e.g., [6, p. 165, Proposition 25]). Assume henceforth that $n^* > 1$. We form the inner product of 1.2 with $\alpha_0, \alpha_1, \ldots$ in turn and then discard a number of terms of the form $(\alpha_i, \alpha_j^*)n_j^*$, $i \neq j$, all $\leqslant 0$. Thus we get

$$
\text{1.6} \qquad \begin{gathered}(\alpha_0, \alpha_0^*)\, n_0^* + (\alpha_0, \alpha_1^*)\, n_1^* \geqslant 0,\\ (\alpha_i, \alpha_{i-1}^*)\, n_{i-1}^* + (\alpha_i, \alpha_i^*)\, n_i^* + (\alpha_i, \alpha_{i+1}^*)\, n_{i+1}^* \geqslant 0 \qquad (1 \leqslant i < q).\end{gathered}
$$

Equality holds only if all the discarded terms are 0. We have $(\alpha_i, \alpha_i^*) = 2$ and

$$
\text{1.7} \qquad \begin{gathered}(\alpha_0, \alpha_1^*) \leqslant -1,\\ (\alpha_i, \alpha_{i+1}) \leqslant -1 \qquad (1 \leqslant i < q).\end{gathered}
$$

Substituting this into 1.6 we get

$$
\text{1.8} \qquad \begin{gathered}2n_0^* - n_1^* \geqslant 0,\\ -n_{i+1}^* + 2n_i^* - n_{i+1}^* \geqslant 0 \qquad (1 \leqslant i < q).\end{gathered}
$$

On adding we get $n_0{}^* + n_{q-1}^* - n_q{}^* \geqslant 0$, hence $n_q{}^* \leqslant n_{q-1}^* + 1$ since $n_0{}^* = 1$. But $n_q{}^* \geqslant n_{q-1}^* + 1$ from the definition of the string. Thus equality holds here and also in all of the above inequalities. Thus all roots of the string have the same length by the equality in 1.7, and all $n_i{}^* = i + 1$ by induction and the equality in 1.8, which proves (a). By the equality in 1.6, α_0 is connected only to α_1, α_i only to α_{i-1} and α_{i+1} for $1 \leqslant i < q$, which proves (b). By (a) and (b), the last expression in (c) is a sum of long roots and its inner product with $\alpha_k{}^*$ is, for $1 \leqslant k < i$ equal to $-(i - k + 1) + 2(i - k) - (i - k - 1) = 0$, for $k = i$ equal to 1, and for $k > i$ equal to 0; hence it equals ω_i, as asserted. In (d), $n_i v_i$ and ω_i are both orthogonal to all α_j ($j \neq i$), hence are in the same line; $n_i v_i = (2/(\alpha_i, \alpha_i))\omega_i$ as we see by taking inner products with α_i. By (c), $\omega_i = \sum \beta_j$, a sum of long roots. Since α_i is also long by (a), we have $n_i v_i = \sum \beta_j{}^* \in L(\sum^*)$, as required.

1.9 *Remark.* The argument used to prove (a) and (b) can be carried one step further to show that if $n^* > 1$, then α_q is a branch point.

1.10 Corollary. (a) *The coefficients $n_i{}^*$ form a connected string of integers starting with* 1 *or with* 2 *and going up.*

(b) *For a prime p, the following conditions are equivalent.*

(1) *$p \leqslant n^*$, the largest $n_i{}^*$.*

(2) *$p =$ some $n_i{}^*$.*

(3) *$p \mid$ some $n_i{}^*$.*

Here (a) follows from 1.5(a), and (b) follows from (a).

1.11 *Remark.* In the same way one may prove an analogous result about $-\alpha_0$ itself and its coefficients n_i and one may add to (b) the condition (4) p is a coefficient of some root. This is because every positive root may be written as a sum of simple roots so that every partial sum is a root.

1.12 Theorem. *Let Σ be a root system and p a prime. Then the following conditions are equivalent.*

(a) *p is a torsion prime for Σ (see* 1.3*).*

(b) *p satisfies any of the equivalent conditions of* 1.10(b) *for some irreducible component of Σ.*

(c) *$L(\Sigma^*)/L(\Sigma_1^*)$ has order p for some maximal closed subsystem Σ_1 of Σ.*

1.13 COROLLARY. *For Σ irreducible of type A_r, C_r, B_r ($r \geqslant 3$), D_r, E_6, E_7, E_8, F_4, G_2, the torsion primes are those $\leqslant n^* = 1, 1, 2, 2, 3, 4, 6, 3, 2$, respectively. If Σ is reducible, its torsion primes are those of its various components.*

This follows from 1.10, 1.12, and a list of highest roots (see, e.g., [6, pp. 200–221]).

To prove 1.12, we may as well assume that Σ is irreducible. If (b) holds, we set $i = p - 1$ in 1.5(a), so that $n_i^* = p$, and also $n_i = p$ since α_i is long. If Σ_1 consists of all roots $\sum m_j \alpha_j$ for which $p \mid m_i$, it readily follows that Σ_1 fulfils the requirements of (c). Clearly (c) implies (a). For the proof that (a) implies (b) and for other purposes, we recall some known facts. We assume Σ irreducible and the other notation as above.

1.14. Let S be the simplex in V defined by $\alpha_i \geqslant 0$ ($1 \leqslant i \leqslant r$), $\alpha_0 \geqslant -1$. Then S is a fundamental domain for W extended by the translations of $L(\Sigma^*)$ acting on V. Hence S projects faithfully into the torus $T = V/L(\Sigma^*)$ and there becomes a fundamental domain for W.

For the proof see either [6, p. 75] or [12, p. 29].

1.15. Let v_i be the vertex of S in V defined as in 1.5(d). Then the roots integral at v_i (or, equivalently, those vanishing at v_i if v_i is projected into T, so that the roots become characters on T) form a closed subsystem Σ_i of rank r. It consists of all roots $\alpha = \sum_{j=1}^{r} m_j \alpha_j$ such that $m_i = 0, \pm n_i$ and has $\{\alpha_j \mid j \neq 0, i\} \cup \{\alpha_0\}$ as a basis.

The last point is proved thus: Let α be as given. If $\alpha > 0$ and $m_i = 0$, then $\alpha = \sum_{j \neq i} m_j \alpha_j$ with each $m_j \geqslant 0$, while if $m_i = -n_i$, then $\alpha = \alpha_0 + \sum_{j \neq i} (m_j + n_j)\alpha_j$, with each $m_j + n_j \geqslant 0$ since $-\alpha_0$ is the highest root.

1.16. The subsystem Σ_i of 1.15 is maximal if and only if n_i is prime. Every maximal subsystem of rank r is, up to conjugacy under W, equal to such a Σ_i.

This is proved in [5], as follows. If n_i is not prime and $p \mid n_i$, then the roots $\sum m_j \alpha_j$ for which $p \mid m_i$ form a larger subsystem because of 1.11. Now let Σ' be any maximal subsystem of rank r. Since $L(\Sigma') \subsetneq L(\Sigma)$, there exists a point v at which Σ' is integral and Σ is not, and this point may be taken in S by 1.14, at a vertex v_i since Σ' has rank r. Then $\Sigma' \subseteq \Sigma_i$ (as in 1.15) and by maximality equality holds, as required.

1.17. If $n_i = 1$, then $\{\alpha_j \mid j \neq i, 0\}$ is a basis of a maximal subsystem, and every maximal subsystem of rank $<r$ is obtained this way.

This is easily verified.

1.18. If $n_i = 1$, in other words, if all roots are integral at v_i, then $\{\alpha_j \mid j \neq 0, i\} \cup \{\alpha_0\}$ is a basis for Σ itself and $-\alpha_i$ is the corresponding highest root.

For $-\alpha_i$ in terms of this basis has the same sum of coefficients as $-\alpha_0$ in terms of the original basis.

Resuming the proof of 1.12, we prove next:

1.19. *Let Σ be irreducible and Σ' a closed irreducible subsystem. Then $n^*(\Sigma') \leqslant n^*(\Sigma)$.*

Let Σ'' be the rational closure of Σ' in Σ. Then every simple system of Σ'' can be extended to one of Σ; for example, by extending it to an arbitrary basis in the usual sense (maximal linearly independent) of Σ and then using the ordering in which the last nonzero coefficient relative to this basis counts. By an obvious induction, this reduces the proof of 1.19 to two cases: (1) that of 1.16; (2) that of 1.17, but with n_i perhaps different from 1. Let $-\alpha_0$, $-\alpha_0'$ be the highest roots of Σ, Σ' with respect to compatible orderings. We express $-\alpha_0' = \sum n_i'\alpha_i'$ in terms of the simple roots of Σ' and these in turn $\alpha_i' = \sum m_{ij}\alpha_j$ in terms of the simple roots of Σ, so that $-\alpha_0' = \sum l_j\alpha_j$ with $l_j = \sum n_i'm_{ij}$. Now every short root must have a short simple root in its support. It follows that $\max n_i'$ (α_i' short) $\leqslant \max l_j \leqslant \max n_j$ (α_j short), and similarly for long roots. Thus if $-\alpha_0'$ is long (as $-\alpha_0$ always is), then the same inequalities hold on the coefficients of $-\alpha_0'^*$ and $-\alpha_0^*$, whence 1.19 holds. This covers case (1) above and leaves the special case of (2) in which two root lengths occur and $-\alpha_0'$ is short. Then α_i must be long, the other simple roots short. Since Σ is indecomposable and $-\alpha_0'$ is a strictly positive combination of the α_j ($j \neq i$), we have $(-\alpha_0', \alpha_i) < 0$. Set $\alpha = \alpha_i - (\alpha_i, -\alpha_0'^*)(-\alpha_0')$, a long root since it equals $w_\beta\alpha_i$ with $\beta = -\alpha_0'$. The coefficients of $\alpha^* = \alpha_i^* + (\alpha_i^*, \alpha_0')(-\alpha_0'^*)$ then dominate those of $-\alpha_0'^*$ and are in turn dominated by those of $-\alpha_0^*$ by 1.1(b), whence 1.19.

Now let p be a torsion prime in 1.12(a). To prove (b), that $p \leqslant n^*$, in view of 1.19, again by induction we are reduced to the two cases just considered. Now in (2) there is no torsion; so (1) must hold. Then by 1.15, $L(\Sigma^*)/L(\Sigma'^*)$ is cyclic of order n_i^*. Thus $p \mid n_i^*$. We have completed the proof of 1.12.

We continue with a technical lemma needed later. We recall that if the notation is as above, then the *central elements* of T (when it is put in as a maximal torus of a semisimple group) are those at which all roots vanish (or, in V above, are integral), or, equivalently, belong to $Z_T(W)$, or yet again (in case Σ is irreducible) those represented in the fundamental simplex S by the origin and the vertices v_i with $n_i = 1$ as in 1.15. These equivalences are all classical [6] and furthermore rather easy to prove.

1.20. LEMMA. *Let Σ be irreducible, p a prime, and t a central element of order p in T, represented in V by the first vertex, v_1, of S.*

(a) *There exist $u \in T$, $w \in W$ such that*

(1) $(1 - w)u = t$.

(2) $u^p \in \langle t \rangle$, *even* $= 1$ *in case* $p \neq 2$.

(3) $w^p = 1$.

(b) *If $p = 2$, then w in* (a) *may be chosen so that if $\beta_1, \beta_2, \ldots$ are the positive roots made negative by w then $1/2 \sum \beta_i^*$ is an integral multiple of v_1.*

Proof. We represent $\langle t \rangle = C$, say, by the corresponding set of p vertices of the fundamental simplex S, and choose u as the centroid of the corresponding face. Then u^p is the product of the elements of C, which is t if $p = 2$ and 1 if p is odd since then the nontrivial elements of C cancel in reciprocal pairs, so that (a2) holds. Now $S - t$ is also one of the standard fundamental cells (cut from T by the equations $\alpha = 0$ for all $\alpha \in \Sigma$) for the action of W on T, hence has the form wS for some $w \in W$. Let $\sigma = w^{-1} \circ \rho_{-t}$, translation by $-t$, so that $\sigma S = S$. Since W acts trivially on C, $\sigma C = C - t = C$, σ fixes the corresponding face of S and hence also its centroid u, so that $w^{-1}(u - t) = u$, $t = (1 - w)u$, and (a2) holds. Then (a3) also holds for $\sigma^p S = S$ implies $w^{-p} S = S$ since t has order p, and then w^{-p} is 1 since it fixes the set of simple roots. Now we claim that (*) w^{-1} as just chosen makes negative just those positive roots with α_1 in their supports. This is known [6, p. 176, Proposition 6] and proved thus. ρ_{-t} maps t and the inequalities defining S there to 0 and those defining wS there. Hence $\{\alpha_0, \alpha_2, \alpha_3 \cdots\}$ is a simple system for the chamber containing wS, and w^{-1} maps it onto $\{\alpha_1, \alpha_2, ...\}$ and also matches up the corresponding lowest roots α_1 and α_0 (see 1.18). Hence w^{-1} keeps positive those positive roots with support in $\{\alpha_2, \alpha_3, ...\}$, i.e., with support not containing α_1. Now let α be positive with α_1 in its support. Write $\alpha = \alpha_1 + \beta$ with $\operatorname{supp} \beta \leqslant \{\alpha_2, \alpha_3, ...\}$. Since $w^{-1} \operatorname{supp} \beta = \operatorname{supp} w^{-1}\beta$ by the above, we have on taking heights that $h(w^{-1}\alpha) = h(w^{-1}\alpha_1) + h(w^{-1}\beta) = h(\alpha_0) + h(\beta) = h(\alpha_0) + h(\alpha) - 1 < 0$ since α_0 is the lowest root. Thus $w^{-1}\alpha < 0$ and (*) holds. Consider now (b), in which $p = 2$ and $w^{-1} = w$. The roots as in (*) are permuted by every w_j $(j \neq 1)$, whence their sum is kept fixed. Hence $1/2 \sum \beta_i^*$ is orthogonal to every α_j $(j \neq 1)$ and so must be a real multiple of v_1, say cv_1. Then $2cv_1 \in L(\Sigma^*)$. Since the order of $v_1 \bmod L(\Sigma^*)$ is 2, we get $2c \in 2\mathbb{Z}$, $c \in \mathbb{Z}$, whence (b).

We close this section by proving some results of de Siebenthal [10], obtained by him by case-by-case verification. Like him, we shall not need them later, but we give proofs since we are set up for them and the only other general proofs in the literature are unnecessarily complicated [4, §4].

1.21. *Let Σ, as above, be a root system and Σ' a proper subsystem of the same rank ordered in some way. Then $s^* = \sum \alpha^*$ $(\alpha \in \sum', \alpha > 0)$ is singular relative to Σ, i.e., orthogonal to some root.*

1.22 *Remarks.* (a) For α a simple root of Σ', $w_\alpha s^* = s^* - 2\alpha$ since w_α permutes the positive roots of Σ' other than α. Hence $\alpha(s^*) = 2$, independent of α, by the formula for a reflection. Hence the line determined by s^* is just "the diagonal" of the given basis of Σ', where all simple roots are equal. Thus 1.21 may be reformulated to say that this diagonal in V is singular. The corresponding result in T is true since s^* can be interpreted as a one-parameter group into T whose image is just the identity component of the diagonal there; looked at this way, it is seen to be true even if T is an algebraic torus. (b) We do not require Σ' to be (integrally) closed (as did the earlier authors) only to satisfy $w_\alpha \Sigma' = \Sigma'$ for all $\alpha \in \Sigma'$. This extra bit of generality actually simplifies our development. For example, Σ' might be the set of short roots of an irreducible root system Σ with two different root lengths and hence not be closed.

Proof of 1.21. Assume not. Then we have an ordering of Σ in which the positive roots are those for which $(s^*, \alpha) > 0$, compatible with the given ordering on Σ' by 1.22 above. Label the simple roots $\alpha_1, \alpha_2, ..., \alpha_r$ of Σ so that $\alpha_1, \alpha_2, ..., \alpha_q$ are those lying in Σ'. Let α be some other simple root of Σ', $\alpha = \sum m_i\alpha_i$. Then $\sum m_i(s^*, \alpha) = 2$. By the choice of α, at least two terms occur on the left. Hence exactly two do and $m_i = 1$, $(s^*, \alpha_i) = 1$ for both of them, so that $\alpha = \alpha_i + \alpha_j$, say, with α_i, α_j not in Σ' and adjacent in the graph of simple roots of Σ. Now these simple roots have a graph which is a forest (no circuits), hence have at most $(r - q - 1)$ adjacent pairs (in fact, exactly $r - q - p$ if p is the number of trees). Hence there are at most $(r - q - 1) + q = r - 1$ roots simple relative to Σ', which must therefore have smaller rank than Σ, a contradiction.

1.23 *Remark.* Even without the assumption of equal rank, s^* in 1.21 is likely to be singular. In fact, by further argument it can be shown that the only case is which s^* is regular when Σ is irreducible is: $\sum$ of type A_r (r even), Σ' any subsystem of rank $r - 1$.

1.24 COROLLARY. *In* 1.21 *above,* $s = \sum \alpha$ $(\alpha > 0,\ \alpha \in \Sigma')$ *is singular relative to* Σ.

To get this we apply 1.21 with Σ, Σ', s^* replaced by Σ^*, Σ'^*, s.

1.25 COROLLARY. *Assume* Σ *irreducible with* $-\alpha_0 = \sum n_i\alpha_i$ *the highest root and* n_1 *prime. Let* v *be the point of* V *at which* $\alpha_0, \alpha_2, \alpha_3, \ldots$ *are all* 1. *Then* α_1 *is also integral at* v, *which is thus central.*

Proof. Let $\Sigma' = \Sigma_1$ as in 1.15, with $\alpha_0, \alpha_2, \alpha_3, \ldots$ as its basis and s^* defined accordingly as in 1.21. Then by 1.21 and 1.22, s^* is a multiple of v and $\alpha(v) = 0$ for some root $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots$ which may be taken positive. We have $0 < a_1 < n_1$ since $\alpha \notin \Sigma'$ clearly. Hence

$$(*) \qquad a_1\alpha_1(v) = -a_2\alpha_2(v) - a_3\alpha_3(v)\cdots \in \mathbb{Z}.$$

But also by the choice of v

$$(**) \qquad n_1\alpha_1(v) = -\alpha_0(v) - n_2\alpha_2(v) - \cdots = -1 - n_2 - n_3 - \cdots \in \mathbb{Z}.$$

Since n_1 is prime, a_1 and n_1 are relatively prime, so that by (*) and (**) $\alpha_1(v) \in \mathbb{Z}$, whence 1.25.

1.26 COROLLARY. *If* $-\alpha_0 = \sum n_i\alpha_i$ *as above and* n_1 *is prime, then* $n_1 \mid h = 1 + \sum n_i$.

This follows from 1.25 and equation (**).

The last two results and their proofs come from [4, §4].

2. Torsion in Reductive Groups

Let G be a (connected) reductive algebraic group over an algebraically closed field k (or else a connected compact Lie group), $G = G_1 T_1$ with G_1 the semisimple component, T_1 the radical, a central torus. We write $F = F(G)$ for the fundamental group of G_1. A reductive subgroup of G will be called *regular* if it contains a maximal torus of G. Its root system may thus (and will) be identified with a subsystem of that of G.

2.1 Definition. A prime p is a *torsion prime* for a reductive group G if $F(G')$ has p-torsion for some regular reductive subgroup G' of G whose root system is integrally closed in that of G.

2.2 *Remarks.* (a) Since every semisimple group is imbeddable in some SL_n, some condition on the allowable subgroups is needed. (b) In the context of compact Lie groups, 2.1 is equivalent to: $H^1(G')$ has p-torsion for some regular subgroup G'. This turns out to be equivalent to: $H^*(G)$ has p-torsion, but at the moment only by a long series of case-by-case considerations (see [1]). (c) The condition on root systems requires further explanation. This will be given below (in 2.9 especially).

Because of the definitions we have:

2.3. Let $G = G_1 T_1$ be as above and G' a regular reductive subgroup.

(a) G and G_1 have the same torsion primes.

(b) The torsion primes of G' are among those of G.

To go further we introduce the data consisting of T, a maximal torus (of G), X its character group, L its lattice of one-parameter subgroups, in natural $\mathbb{Z}$-duality with X, and Σ the root system. We have Σ imbedded in X and Σ^* in L.

2.4. *We have* $F = F(G) = \operatorname{tors} L/L(\Sigma^*)$.

If G is semisimple, this may be taken as the definition of F. (If we write F_s for the separable part of F, of order prime to char k, and F_i for the inseparable part, of order a power of char k, so that $F = F_s F_i$, then F_s is isomorphic to the kernel of the universal covering $\pi\colon G' \to G$, while $F_i \neq \{1\}$ signifies that $\ker d\pi \neq 0$, i.e., that π is not separable.) In particular, $L = L(\Sigma^*)$ is the condition for simple connectedness. If G is arbitrary, T can be written as the direct product of a maximal torus of G_1 and another torus, so that 2.4 still holds.

2.5 LEMMA. *If G is reductive, then its torsion primes are those of its root system Σ (see* 1.3) *together with those of its fundamental group F, i.e., those of $L/L(\Sigma^*)$.*

Proof. We may assume G semisimple. Clearly the torsion primes of F are torsion for G. So are those of Σ for if p is one of them then by [8, Exp. 17] we may choose G' as the subgroup corresponding to $\Sigma' = \Sigma_{p-1}$ (see 1.15 and 1.5(a)) to get p-torsion in $L(\Sigma^*)/L(\Sigma'^*)$, hence also in $L/L(\Sigma'^*) = F(G')$. Conversely, let p be a torsion prime. Then $L/L(\Sigma'^*)$ has p-torsion for some $\Sigma' = \Sigma(G')$ with G' as in 2.1, so that either $L(\Sigma^*)/L(\Sigma'^*)$ does, i.e., Σ does, or else $L/L(\Sigma^*)$ does, i.e., F does, as required.

2.6 COROLLARY. *If G_1 is simply connected, then its torsion primes are those of its root system.*

2.7 COROLLARY. *If G is simple, then it can have p-torsion beyond that of its root system only in the cases: type A_r, $p \mid (r+1)$; type C_r, $p = 2$.*

Proof. The possibilities for F in the various cases are, of course, well known.

2.8 COROLLARY. *Each torsion prime for G divides the order of the Weyl group (but not conversely).*

Proof. We may assume G simple, adjoint, of rank r, say. By a formula of Weyl $|W| = f \cdot r! \cdot \Pi n_i$ with $f = |F|$ and $\sum n_i\alpha_i$ the highest root. Since $n_i{}^*$ divides n_i, the corollary follows from 1.12.

2.9 LEMMA. *Let G and Σ be as above.*

(a) *Every closed subsystem of Σ supports a regular reductive subgroup of G.*

(b) *If Σ' is the root system of a regular reductive subgroup and Σ'' its (integral) closure in Σ, then $\Sigma' \neq \Sigma''$ only if* $\operatorname{char} k = p \neq 0$ *and p is the square-length ratio of two elements in the same component of Σ''. In that case, $L(\Sigma''^*)/L(\Sigma'^*)$ is an elementary p-group.*

2.10 *Remark.* This shows that the extra condition on root systems of 2.1 is needed only in the rather exceptional circumstances of (b). It has no bearing in the present section since G has no semisimple elements of order p, but does so in the next section where elements of the Lie algebra are considered.

Proof. Here (a) is standard [8, Exp. 17]. In (b) we may assume that $\Sigma'' = \Sigma$, that $\Sigma \neq \Sigma'$, and that Σ is irreducible so that there are at most two root lengths. Hence there exist $\alpha, \beta \in \Sigma'$ such that $\alpha + \beta \in \Sigma - \Sigma'$. Then (*) $(\alpha, \beta) \geqslant 0$ since otherwise $\alpha + \beta$ would equal either $w_\alpha \beta$ or $w_\beta \alpha$ and hence be in Σ'. Then by (*) $\alpha + \beta$ is longer than α and β so that (**) $\alpha + \beta$ is long, α and β short. Further, $\alpha + 2\beta$ is longer than $\alpha + \beta$ so that it cannot be a root. If q is the smallest nonnegative integer such that $\beta - q\alpha$ is not a root, then by symmetry $\beta - q\alpha = w_\alpha(\beta + 2\alpha)$, so that $q = (\beta, \alpha^*) + 2 = |\alpha + \beta|^2/|\alpha|^2$ by (**). Now if U_α, U_β are the one-parameter unipotent subgroups corresponding to α, β, then (U_α, U_β) (commutator) $\subseteq \Pi\, U_{i\alpha+j\beta}$ $(i, j \geqslant 0)$ and $U_{\alpha+\beta}$ is present on the right unless q above is 0 in k. Hence $|\alpha + \beta|^2/|\alpha|^2 = q = 0$ in k. However, $|\alpha + \beta|^2/|\alpha|^2 = 2$ or 3, a prime. Hence $q = p$. Now if $\{\alpha_i\}$ is a basis for Σ' and $\alpha = \sum m_i \alpha_i$ $(m_i \in \mathbb{Z})$ is any root of Σ, then $\alpha^* = \sum m_i^* \alpha_i^*$ with $m_i^* = m_i |\alpha_i|^2/|\alpha|^2 \in q^{-1}\mathbb{Z} = p^{-1}\mathbb{Z}$. Thus $L(\Sigma^*)/L(\Sigma'^*)$ is an elementary p-group, which proves (b).

We continue with a final preliminary result.

2.11. Let G' be a regular reductive subgroup of G and Σ' its root system. Then the following conditions are equivalent.

(a) The natural map $F(G') \to F(G)$ is injective.

(b) $L(\Sigma^*)/L(\Sigma'^*)$ has no torsion.

(c) Every long root of Σ rationally dependent on Σ' is in Σ'.

The equivalence of (a) and (b) follows rather easily from 2.4. Now assume (b). Let α be a root as in (c). Then by (b) $\alpha^* = \sum \beta_i^*$ $(\beta_i \in \Sigma')$. We observe now as in the proof of 2.9 that (*) if $\beta, \gamma \in \Sigma'$, $(\beta, \gamma) < 0$, then $\beta + \gamma \in \Sigma'$. Hence if the above expression for α^* is minimal, then $(\beta_i, \beta_j) \geqslant 0$ for all i, j. Then since α is long, hence α^* short, there can be only one summand, so that $\alpha = \beta_1 \in \Sigma'$, which is (c). Now if Σ'' is the rational closure of Σ' in Σ, then $L(\Sigma^*)/L(\Sigma''^*)$ has no torsion (since a basis of Σ'' can be extended to one of Σ). Thus in proving that (c) implies (b) we may assume that $\Sigma'' = \Sigma$ and then must show that $L(\Sigma'^*) = L(\Sigma^*)$ (but not that $\Sigma' = \Sigma$: consider, e.g., $\Sigma' = \{$long roots$\}$ in a two root length system). If α is a long root in Σ, then α^* is short and in Σ'^* by assumption. Since Σ^*, like any root system, is generated by its short roots, we get $L(\Sigma'^*) = L(\Sigma^*)$, as required.

2.12 Definition. If any of the equivalent conditions of 2.11 hold, we shall say that G' is *simply connected in* G.

2.13 *Remarks.* (a) The relation just defined is transitive. (b) If G (or rather its semisimple component) is simply connected and G' is simply connected in G, then G' is simply connected. (c) If (b) of 2.11 fails, we still have a homomorphism $F(G') \to F(G)$, the kernel being tors $L(\Sigma^*)/L(\Sigma'^*)$. (d) If Σ' above is rationally closed in Σ, then G' is simply connected in G (e.g., a Levi component of a parabolic subgroup is such). (e) If G' is simply connected in G, then Σ' is (integrally) closed in Σ. For (*) above implies that any short root integrally dependent on Σ' is in Σ'.

We turn now to one of our main concerns, centralizers of semisimple elements. First we recall some facts from [12, §7].

2.14 Lemma. *Let G be reductive, T a maximal torus, t an element or subset of T, Σ' the (closed) subsystem of roots vanishing at t, W' its Weyl group, and W'' the centralizer of t in W.*

(a) *$Z_G(t)$ is generated by T, those U_α such that $\alpha \in \Sigma'$, and those n_w such that $w \in W''$.*

(b) *$Z_G(t)^0$ is generated by T and the U_α's alone. It is (regular) reductive with Σ' as its root system.*

(c) *W' is normal in W'' and $Z_G(t)/Z_G(t)^0$ is isomorphic to W''/W'.*

We are using the notation of [12] for algebraic groups, except that U_α, not X_α, denotes the unipotent group corresponding to α. Here (a) comes from the Bruhat lemma [12, 6.3] and then everything else from the easily proved fact that W'' fixes Σ'. (If G were a compact Lie group instead, then a corresponding result would hold with $\langle U_\alpha, U_{-\alpha}\rangle$ replaced by an analogous compact group, SL_2 by SU_2 most of the time.)

We observe that $Z_G(t)^0$ fulfils the conditions of 2.1.

As a consequence of 2.14 we have:

2.15 Theorem. *If G is simply connected and t a single semisimple element, then $Z_G(t)$ is connected.*

The point is that $W'' = W'$ in 2.14(c), a geometric property of reflection groups acting suitably on tori, which is proved in [12, §5] and also in [3, pp. 36–37] in a more direct way. For compact Lie groups, a different proof may be found in [1, p. 225].

From 2.15 one can deduce:

2.16 COROLLARY. *Assume G reductive but perhaps not simply connected, t as in* 2.14.

(a) *$Z_G(t)/Z_G(t)^0$ is isomorphic to a subgroup of $F_s(G)$. Every subgroup is attainable.*

(b) *If $t^n \in Z(G)$, then $y^n = 1$ for every $y \in Z_G(t)/Z_G(t)^0$.*

(c) *In* (b), *if n is prime to $|F_s|$, then $Z_G(t)$ is connected.*

Here (a) and (b) (with the assumption $t^n = 1$) follow from [12, 9.1 and argument of 9.11] for semisimple groups, but the transition to reductive groups is immediate. Then (c) follows from (b). Observe that (a) provides both an extension and a converse for 2.15. In particular, $Z_G(t)$ is always connected if the universal covering of the semisimple component of G is purely inseparable.

What happens if we consider several semisimple elements?

2.17 LEMMA. *Assume in* 2.14 *that t is a subtorus of T. Then $Z_G(t)$ is connected and it is simply connected in G* (*see* 2.12).

Proof. The connectivity is a standard fact [8, Exp. 6, Theorem 6]. Since t is now a divisible group, Σ' is rationally closed in Σ and the second assertion holds by 2.13(d).

2.18 COROLLARY. *Let A be a solvable* (*not necessarily closed*) *subgroup of semisimple elements of G* (*still reductive*).

(a) *$Z_G(A)^0$ is reductive.*

(b) *$Z_G(A)/Z_G(A)^0$ is solvable, consists of semisimple elements, and its torsion primes* (*those that divide its order*) *are among those of $A/A^0 \cdot (A \cap Z(G))$.*

(c) *If A/A^0 is nilpotent, then so is $Z_G(A)/Z_G(A)^0$.*

Proof. A^0 is connected and solvable, hence contained in a Borel subgroup, hence in a torus [8, Exp. 6, Lemma 1], so that $\bar{A}^0$ is a torus. In view of 2.17 and the fact that $\bar{A}$ splits over $\bar{A}^0$ (which is divisible), we may replace G by $Z_G(A^0)$ and A by A/A^0 and thus assume that A is finite. In that case we shall prove a somewhat stronger statement.

2.19. *In* 2.18 *let A be replaced by a finite solvable group of semisimple automorphisms of G, $Z_G(A)$ by G_A* (*the group of fixed points*), *and $A/A^0 \cdot (A \cap Z(G))$ by A. Then the conclusions there hold.*

This reduces to 2.18 in case the automorphisms are all inner. Assume first that $A = \langle \sigma \rangle$, a cyclic group, of order m say. Then by [12, 8.1 and proof of 9.1] (a) holds if G is semisimple, hence also if G is reductive, and (b) holds if G is semisimple. Consider (b) in case $G = T$, a torus. Replacing T by $T/T_\sigma{}^0$, we may assume T_σ $(= \ker(1 - \sigma))$ finite, hence $(1 - \sigma)$ surjective on T, hence injective on $X = X(T)$. Then T_σ is in duality with the subgroup of $X/(1 - \sigma)X$ consisting of the elements of order not divisible by char k. Now $X/(1 - \sigma)X$ has order $\det_X(1 - \sigma)$, and σ has on X a characteristic polynomial which is a product of cyclotomic polynomials $\varphi_d(t)$ $(d \mid m, d > 1)$. Thus $\det(1 - \sigma)$ is a product of $\varphi_d(1)$'s. However, $\varphi_d(1)$ is p if d is a power of a prime p, is 1 otherwise. Thus if p is torsion for $T_\sigma = T_A$, it is torsion for some d, hence for A, and (b) holds. Now let G be reductive, $G = ST$, with S semisimple and T the radical, a torus. Set $H = S \times T$, $\pi \colon H \to G$ the natural map, and $F = \ker \pi$, a finite central subgroup. We use the exact sequence of cohomology [9, p. 133, Proposition 1] $H_A \to^{\pi} G_A \to^{\delta} H^1(A, F)$. Here $\pi H_A{}^0 = G_A{}^0$ and $G_A{}^0 \subseteq \ker \delta$ since $H^1(A, F)$ is finite. Thus H_A may be replaced by $H_A/H_A{}^0$ and G_A by $G_A/G_A{}^0$. Now $H_A/H_A{}^0$ satisfies (b) by what has been proved for semisimple groups and for tori, and $H^1(A, F)$ does also [9, p. 138, Corollary 1]. Hence so does $G_A/G_A{}^0$. Thus (b) holds in case A is cyclic. Consider now the general case. Let A' be a proper nontrivial normal subgroup of A. We have $G_A \supset G_A \cap G^0_{A'} \supset G_A{}^0$. The first quotient is isomorphic to a subgroup of $G_{A'}/G^0_{A'}$ and the second equals $K_{A''}/K^0_{A''}$ with $K = G^0_{A'}$ and $A'' = A/A'$. Thus (b) follows by induction, and so does (a) since $G_A{}^0 = (K_{A''})^0$, clearly. If A is nilpotent and p a prime, we choose A' to be the complement of a Sylow p-subgroup of A. Then from what has been proved, the first quotient above is a p'-group, the second a p-group, so that $G_A/G_A{}^0$ has a normal Sylow p-subgroup. Since p is arbitrary, $G_A/G_A{}^0$ is nilpotent, which proves (c).

2.20 *Example.* If A/A^0 is Abelian in 2.18(c), then $Z_G(A)/Z_G(A)^0$ need not be Abelian. Let G be adjoint of type D_4 in char $\neq 2$ and A the subgroup of T defined by $\alpha_1 = \alpha_2 = \alpha_3 = \pm 1$, $\alpha_4 = \pm 1$, in terms of a root basis for which α_4 is at the center of the Dynkin diagram. The following may be verified. A is a (2, 2) group consisting of the identity and three involutions conjugate to one another. No root vanishes on A. Thus $Z_G(A)/Z_G(A)^0$ is isomorphic to $Z_W(A)$ by 2.14(c). Let R be the root lattice, R' the sublattice vanishing on A. Then A is dual to R/R' and $Z_W(A) = Z_W(R/R')$. To find the latter group, write $\alpha_1 = x_1 - x_2$,

$\alpha_4 = x_2 - x_3$, $\alpha_2 = x_3 - x_4$, $\alpha_3 = x_3 + x_4$ in terms of basis of $\mathbb{Z}^4$. Then R is the sublattice in which the sum of the coordinates is even, R' the one in which all coordinates have the same parity. W acts on the x's via sign changes, even in number, combined with arbitrary permutations. All such sign changes lie in $Z_W(R/R')$, but only the permutations of the Klein (2, 2) group do. The group $Z_W(R/R')$ is not Abelian since, for example, the permutation (13)(24) does not fix the change of sign of the first two coordinates. $Z_W(A)$ is in fact the "metaplectic group" of the (2, 2) group.

We come back now to the torsion primes.

2.21 THEOREM. *Let G be reductive, t a semisimple element, and n an integer such that $t^n \in Z(G)$. Then the torsion primes of $L(\Sigma^*)/L(\Sigma'^*)$ (with Σ, Σ' as in* 2.14) *all divide n.*

2.22 COROLLARY. *If no torsion prime for Σ divides n, then $Z_G(t)^0$ is simply connected in G.*

This follows from 1.3 and 2.21. In view of 2.13(b), it implies Theorem 0.1 of the introduction.

Proof of 2.21. We may assume G semisimple, then simply connected by going to the covering group, then simple since G is at this stage a product of simple groups. In that case we prove a sharper result:

2.23. *If G in* 2.21 *is simple, then* $|\operatorname{tors} L(\Sigma^*)/L(\Sigma'^*)|$ *divides n.*

Proof. By 2.9(a) we may assume that Σ itself is the rational closure of Σ' in Σ. We consider the compact torus $T^c = \mathbb{R} \otimes L/L$ (L is the lattice of one-parameter subgroups of T) for which L and X have the same interpretations as they do for T. Since G is simply connected, $L = L(\Sigma^*)$, so that T^c is just the torus labeled T in 1.14. By [12, 5.1] there exists $t^c \in T^c$ such that the same characters vanish at t^c and at t. Since all roots vanish at t^n and $\alpha(t^n) = 0$ is equivalent to $(n\alpha)(t) = 0$, it follows that all roots vanish at $(t^c)^n$. Now t^c is equivalent to a point of the fundamental domain S of 1.14, to a vertex since Σ' and Σ have the same rank, to a vertex other than 0 since otherwise $\Sigma' = \Sigma$ and we are done, hence to some v_i as in 1.15; and then $\Sigma' = \Sigma_i$. Now $\alpha(mv) = 0$ in T is equivalent to $\alpha(mv) \in \mathbb{Z}$ in the covering space V above. Hence $n_i v_i$ is the smallest multiple of v_i at which all roots vanish. Hence n is a multiple of n_i, which in turn is a multiple of n_i^* since

$n_i/n_i^* = (\alpha_0, \alpha_0)/(\alpha_i, \alpha_i)$, an integer since α_0 is a long root. Since $L(\Sigma^*)/L(\Sigma_i^*)$ has order n_i^* by 1.15, we are done.

A number of the results so far may be put together as follows.

2.24 THEOREM. *Let G be reductive, A a subgroup of T, X^0 the annihilator of A in X, and p a prime. If X/X^0 has no p-torsion or if $A/A^0 \cdot (A \cap Z(G))$ has none or if G has none, then $Z_G(A)/Z_G(A)^0$ and $L(\Sigma^*)/L(\Sigma'^*)$ have none.*

Proof. As is easily seen, the first assumption implies the second. Thus there remain four results to be proved. We label them 11, 12, 21, 22. Then 11 follows from 2.18(b) and 22 from 1.3 and 2.5. For 21 and 12 we may, as earlier, assume that A is finite. Then 21 and 12 follow from 2.5, 2.16(a), and 2.21 in case A is cyclic, hence in general by an obvious induction.

2.25 COROLLARY. *Let G be reductive and A a commutative subgroup of semisimple elements. Write $A/A^0 \cdot (A \cap Z(G))$ as a product of, say a cyclic subgroups, and let exactly b of these have torsion in common with G.*

(a) *If $b \leqslant 1$, then A is contained in a torus.*

(b) *If $b = 0$, then in addition $Z_G(A)$ is connected and simply connected in G.*

(c) *If G is simply connected, then the values of b in* (a) *and the first part of* (b) *may be increased by* 1.

Proof. By 2.17, we may assume A finite and then eliminate the cyclic subgroups having no torsion in common with G, thus assume that $a = b$. Then (b) is obvious and (a) also since every semisimple element is contained in some torus. If G is simply connected and C is one of the cyclic subgroups still remaining, then we may apply (a) and (b) as already proved with $Z_G(C)$ in place of G, by 2.15, to get (c).

2.26 *Examples.* (a) In SL_n or Sp_n there are no torsion primes. Thus every commuting set A of semisimple elements can be put in a torus and has a connected centralizer, a classical result. (b) In SO_n the only torsion prime is 2, by 2.5. Thus the conclusions of (a) hold if A/A^0 is of odd order, and in any case $Z_G(A)/Z_G(A)^0$ is a 2-group by 2.24.

In the last example, the diagonal elements of order 2, which cannot be imbedded in any torus, show that the assumption there is essential. Such examples, consisting of elementary p-groups, exist whenever p is a torsion prime, as we shall now show. More specifically, we shall prove the following two theorems.

2.27 THEOREM. *Let G be reductive and p a prime different from* char k. *Then the following conditions are equivalent.*

(a) $p \nmid |F|$ (*F is the fundamental group of G*).

(b) *$Z_G(t)$ is connected for every element t of order p or, equivalently, for every* rank 1 *elementary p-subgroup.*

(c) *Every* rank 2 *elementary p-subgroup is contained in a torus.*

2.28 THEOREM. *Let G and p be as in 2.27. Then the following conditions are equivalent.*

(a) *p is not a torsion prime for G.*

(b) *$Z_G(P)$ is connected for every* rank $\leqslant 2$ *elementary p-subgroup P.*

(c) *$Z_G(P)$ is connected for every elementary p-subgroup P.*

(d) *Every* rank $\leqslant 3$ *elementary p-subgroup P is contained in a torus.*

(e) *Every elementary p-subgroup P is contained in a torus.*

Proof. In 2.27, (a) implies (b) by 2.16(a) or 2.24, while if (b) holds and t_1, t_2 generate P as in (c), then any maximal torus of $Z_G(t_1)$ containing t_2 will do in (c), leaving only "(c) implies (a)" to be proved. Consider now 2.28. Here (a) implies (c) (and (e)) by 2.16(a,b) or 2.24, while (c) implies (b) and (e) implies (d) trivially. Consider now (c_i), (e_i) obtained from (c), (e) by sticking to subgroups of rank i. Then (c_i) implies (e_{i+1}) for every i as in the proof that (b) implies (c) in 2.27, which is just the case $i = 1$. Thus (c) implies (e) and (b) implies (d), and only "(d) implies (a)" remains here. To prove the remaining assertions, we may assume G semisimple. We use the following two lemmas.

2.29 LEMMA. *Let G be simply connected and p a torsion prime for G other than* char k. *Then there exists an element t of order p such that*

(a) *$Z_G(t)$ is semisimple.*

(b) *Both the center and the fundamental group of $Z_G(t)$ have elements of order p.*

2.30 LEMMA. *Let G be as in 2.29, p any prime, and t an element of order p of the center of G. Then there exist elements u, v of G such that*

(a) $(u, v) = t$.

(b) *$u^p, v^p \in \langle t\rangle$, even $= 1$ in case p is odd.*

Assume these lemmas for a moment. Suppose in 2.27 that (a) fails. We must show that (c) also fails. Let $\pi: G' \to G$ be the universal covering. Choose $t \in \ker \pi$ of order p and then u and v as in 2.30. Then $(\pi u)^p = 1$, $(\pi v)^p = 1$, and $\pi u, \pi v$ cannot be put into the same torus T of G since then $\pi^{-1}T$ would be a torus in G', hence an Abelian group, containing u, v, a contradiction since $(u, v) = t \neq 1$. Thus (c) fails and 2.27 is completely proved. Now assume that (a) fails in 2.28. If $p \nmid |F|$, we choose t as in 2.29, while if $p \mid |F|$, we set $t = 1$. Thus in both cases $Z_G(t) = G_1$, say, is a semisimple group for which 2.27(a) fails. Thus 2.27(c) also fails and there is a rank-2 elementary p-subgroup P of G_1 not contained in any torus of G_1. Then $\langle P, t\rangle$ has rank $\leqslant 3$ and is not contained in any torus of G, for any such torus would have to centralize t and thus be contained in G_1. Thus (d) fails. In other words, (d) implies (a) in 2.28 and that theorem is also proved, mod 2.29 and 2.30.

2.31 *Remark.* We may replace the inequality in (b) of 2.28 by an equality since P above always has rank 2, and in case $p \nmid |F|$ do the same in (d) by 2.27.

It remains to prove 2.29 and 2.30. We recall the basic transfer situation of [12, 5.1]. Let $G, T, X, L, W, \ldots$ be as at the beginning of this section. Let $V = \mathbb{R} \otimes_{\mathbb{Z}} L$ and $T^c = V/L$, a compact torus. Then X may be viewed as the character group of T^c.

2.32 LEMMA. *Let ψ be a fixed (unnatural) isomorphism of* tors k^* *into* $\mathbb{R}/\mathbb{Z}$ *and* φ *its extension from* tors $T =$ tors $k^* \otimes L$ *to* tors $T^c =$ tors $\mathbb{R}/\mathbb{Z} \otimes L$. *Then φ is a W-isomorphism and for any subset S of* tors T *the annihilators of S and $\varphi(S)$ in X are equal.*

Proof. The first point holds because the two actions of W are extensions of that on L, and the second because φ is injective.

Proof of 2.29 *and* 2.30. We have $L = L(\Sigma^*)$ since G is simply connected, so that the torus T^c of 2.32 is just the torus of 1.14, labeled T there. In 2.29 we choose $t \in T$ so that $\varphi(t) \in T^c$ is just the ith vertex of S, $i = p - 1$, as in 1.5(d). Then $Z_G(t)$ is connected reductive by 2.15, and the roots vanishing at t form the system Σ_i of 1.15, of the same rank as Σ, so that $Z_G(t)$ is semisimple. It contains t, of order p by 1.5(a,d) and 2.32, in its center, and has $L(\Sigma^*)/L(\Sigma_i^*)$, i.e., $\mathbb{Z}/p\mathbb{Z}$, as its fundamental group. Thus 2.29 is proved. Now let t be as in 2.30. By 2.32, $\varphi(t)$ has order p and is in "the center" of T^c. We choose $\varphi(u)$, w accordingly as in 1.20 and then shift back to u, $w \in T$, W via 2.32. The equations (a1, a2) of 1.20 continue to hold, and it remains to show that w can be represented in $N(T)$ by a v for which 2.30(b) holds. For each simple root α, we choose n_α to represent w_α in $N(T)$ and to be in the corresponding rank-1 subgroup of G (isomorphic to SL_2 in the present case, to SU_2 if G were a compact Lie group). Let $w = w_1 w_2 \cdots w_s$ be a minimal expression as a product of simple reflections. Provisionally, we set $v = n_1 n_2 \cdots n_s$, the corresponding product of n_α's.

(1) If α and β are distinct simple roots, then $n_\alpha n_\beta n_\alpha \cdots = n_\beta n_\alpha n_\beta \cdots$ (ord $w_\alpha w_\beta$ terms on each side). For by grouping the terms correctly one can show that the ratio of the two sides is in $\operatorname{Im} \alpha^*$ and also in $\operatorname{Im} \beta^*$, hence is 1 since $\{\alpha^*, \beta^*\}$ is part of a basis of L (cf. [11, Lemma 56(a)]).

(2) The value of v is independent of the minimal expression chosen for w. As is known, any minimal expression for w can be transformed into any other as a consequence of the relations in (1) with w's in place of n's. Hence (2) follows from (1).

(3) $n_\alpha^2 = \alpha^*(-1)$, an element of order 2, for every simple α. For it is known that there exists a homomorphism of SL_2 into G which maps the off-diagonal matrix $(0, 1; -1, 0)$ onto n_α and $\operatorname{diag}(a, a^{-1})$ onto $\alpha^*(a)$ for all $a \in k^*$.

(4) In the group generated by the chosen n_α's those elements that lie in T all have order 1 or 2. Let $n = n_1 n_2 \cdots n_q$ be one such. Then correspondingly $w_1 w_2 \cdots w_q = 1$. Now any relation in W is a consequence of those mentioned in (2) and the relations $w_\alpha^2 = 1$. It follows from (3), e.g., by induction on q, that n can be written as a product of $\alpha^*(-1)$'s ($\alpha \in \Sigma$), whence (4).

We return to the proof of 2.30. Since $w^p = 1$, v^p is in T, hence has order 1 or 2 by (4). If p is odd and v^p has order 2, we replace v by $v' = v^{p+1}$ and then have $v'^p = (v^p)^{p+1} = 1$, i.e., 2.30(b) since $p + 1$ is even. Assume now that $p = 2$. Then $w = w^{-1}$ so that $v^2 = n_1 n_2 \cdots n_s \cdot n_s \cdots n_2 n_1$ by (2). By (3) this may be simplified from the center outward to yield $v^2 = \Pi \beta_i^*(-1)$ with the product over all $\beta_i = w_1 w_2 \cdots w_{i-1} \gamma_i$ with γ_i denoting the simple root corresponding to w_i $(1 \leqslant i \leqslant s)$, i.e., over all positive roots made negative by w [6, p. 158, Corollary 2]. Now each $\alpha_i^*(-1)$ (α_i simple) is characterized in T or in T^c by the equations $\omega_j(\alpha_i^*(-1)) = (-1)^{\delta_{ij}}$ with $\{\omega_j\}$ as in 1.5(c). Hence by 2.32 it will be enough to show that $\varphi(v^2) = \Pi \beta_i^*(-1)$ (in T^c) is a multiple of $\varphi(t)$. In the covering space V of T^c in which

$\beta_i^*(-1)$ may be represented by $1/2\beta_i^*$, this amounts to showing that $1/2\sum\beta_i^*$ is a multiple of v_1 representing t in V. Since this has been done in 1.20(b), we are done with 2.30, hence also with 2.27 and 2.28.

2.33 *Remark.* It seems likely to us that the replacement $v \to v^{p+1}$ above is unnecessary and that u and v as chosen originally are in fact conjugate.

There is one more item to be discussed in this section.

2.34 COROLLARY. *Let G be reductive, G_1 and G_2 reductive subgroups containing the same maximal torus T and corresponding to integrally closed subsystems of roots (which is automatic most of the time by 2.9(b)). Then $(G_1 \cap G_2)^0$ is reductive and $(G_1 \cap G_2)/(G_1 \cap G_2)^0$ is nilpotent and its torsion is contained in that of Σ.*

2.35 LEMMA. *Let Σ_1, Σ_2, W_1, W_2 be the root systems, Weyl groups of G_1, G_2. The $G_1 \cap G_2$ is generated by T, those U_α such that $\alpha \in \Sigma_1 \cap \Sigma_2$, and those n_w such that $w \in W_1 \cap W_2$; and $(G_1 \cap G_2)^0$ by T and the U_α's alone. The Weyl group W_3 of $\Sigma_1 \cap \Sigma_2$ is normal in $W_1 \cap W_2$ and $(G_1 \cap G_2)/(G_1 \cap G_2)^0$ is isomorphic to $(W_1 \cap W_2)/W_3$.*

Proof. An element of $G_1 \cap G_2$ has three Bruhat decompositions, one in G, one in G_1, one in G_2, which must be identical. From this, 2.35 readily follows.

Proof of 2.34. By the lemma, $(G_1 \cap G_2)^0$ is reductive. Since W_1, W_2, W_3 depend only on Σ_1, Σ_2, we may be 2.9 switch to any group with Σ as its root system, thus assume that (*) G is semisimple, simply connected and of char 0. Set $A_1 = Z_T(\Sigma_1)$. Then $\Sigma_1 = Z_\Sigma(A_1)$ since Σ_1 is integrally closed. Hence $G_1 = Z_G(A_1)^0$ by 2.14, and similarly $G_2 = Z_G(A_2)^0$. We have $Z_G(A_1A_2) \supset G_1 \cap G_2 \supset (G_1 \cap G_2)^0 = Z_G(A_1A_2)^0$, the last equality by 2.14(b) and 2.35. We conclude by applying 2.18, 2.24, and 2.6 to the outside terms.

2.36 *Complements.* (a) Conversely, every torsion prime p for Σ can be realized in 2.34. For assuming as we may that (*) above holds, we may choose u, v of order p in T so that $Z_G(u, v)$ is disconnected by 2.28 and then set $G_1 = Z_G(u)$ and $G_2 = Z_G(v)$. (b) If Σ_1, Σ_2 are rationally closed in Σ, then $G_1 \cap G_2$ is connected. For in this case we may take $A_1 = Z_T(\Sigma_1)^0$ and similarly for A_2 and then use the fact that A_1A_2, a torus, has a connected centralizer. (c) As an example, we see that if G is of type A_n or C_n in 2.34, then $G_1 \cap G_2$ is always connected.

A final remark: The results and proofs of this section hold equally well for (connected) compact Lie groups, subject to minor modifications that have been indicated from time to time (cf. [1]).

3. The Infinitesimal Case

In this section we carry over our earlier results, especially 2.27 and 2.28 (see 3.13 and 3.14 below), to semisimple elements of $\mathfrak{g}$, the Lie algebra of G.

3.1 The Lie algebra of a torus. Let T be an algebraic torus over k with L and X as before. Then T may be identified with $k^* \otimes_{\mathbb{Z}} L$. This is clear if the rank is 1 since $k^* \otimes_{\mathbb{Z}} \mathbb{Z} = k^*$ and then if the rank is arbitrary as we see by taking direct products. Explicitly, $\sum c_i \otimes \lambda_i \sim \Pi\, \lambda_i(c_i)$ if the elements of L are considered to be one-parameter subgroups. The Lie algebra $\mathfrak{t}$ of T then becomes $k \otimes_{\mathbb{Z}} L$ since that of k^* is k. For each χ in X, there is then a linear function on $\mathfrak{t}$, the differential of χ, also to be denoted χ, which sends $\sum c_i \otimes \lambda_i$ to $\sum c_i(\lambda_i\,, \chi)$. Thus $\mathfrak{t}$ comes with a natural $\mathbb{Z}$-structure, hence with a natural structure of variety over k_0, the prime field. As is easily seen, H in $\mathfrak{t}$ is in $\mathfrak{t}(k_0) = k_0 \otimes L$ if and only if $X(H) \subseteq k_0$.

3.2 *Example.* Assume that T above is a maximal torus of a simply connected semisimple algebraic group, so that the simple coroots $\{\alpha_i^*\}$ form a basis for L and their images $\{1 \otimes \alpha_i^*\}$ one for the k_0-structure of $\mathfrak{t}$. If $\{\omega_j\}$ is the dual basis of X consisting of the fundamental weights, then $\omega_j(1 \otimes \alpha_i^*) = \delta_{ji}$. Thus $1 \otimes \alpha_i^*$ is just that element of $\mathfrak{t}$ which in the classical theory is denoted H_{α_i}, and similarly for every root α.

We recall that a subalgebra of the Lie algebra of an algebraic group is said to be *algebraic* if it is the Lie algebra of an algebraic subgroup.

3.3 Lemma. *If T, $\mathfrak{t}$, etc. are as above and $\mathfrak{t}_1$ is a subalgebra of $\mathfrak{t}$, then the following are equivalent.*

(a) *$\mathfrak{t}_1$ is an algebraic subalgebra of $\mathfrak{t}$.*

(b) *$\mathfrak{t}_1 = k \otimes L_1$ for some sublattice L_1 of L such that L/L_1 has no torsion.*

(c) $\mathfrak{t}_1$ *is defined over* k_0, *the prime field.*

(d) $\mathfrak{t}_1$ *has a basis of elements of* $\mathfrak{t}(k_0)$.

Proof. If $\mathfrak{t}_1$ in (a) is the Lie algebra of the subtorus T_1, then the corresponding lattice L_1 satisfies (b) since if $\lambda \in L$ and $n\lambda \in L_1$, then $\operatorname{Im} \lambda = \operatorname{Im} n\lambda \subseteq T_1$, whence $\lambda \in L_1$. Thus (a) implies (b). If (b) holds, then a basis of L_1 can be extended to one of L. It then follows, from uniqueness of expression in terms of a basis, that $T_1 = k^* \otimes L_1$ is a subtorus of T with Lie algebra $\mathfrak{t}_1$. Thus (b) implies (a). If $\{\lambda_i\}$ is a basis of L_1 as in (b), then $\{1 \otimes \lambda_i\}$ is one for $\mathfrak{t}_1$. Thus (b) implies (d). That (d) is equivalent to (c) is a standard (elementary) fact from Galois theory which holds for arbitrary fields and vector spaces. Finally, assume $\mathfrak{t}_1$ has a basis as in (d). If $\sum c_i \otimes \lambda_i \in k_0 \otimes L$ is in the basis, it may be written $c \otimes \lambda$ since the c_i's are all rational numbers and may be taken to a common denominator. Thus the basis may be taken in the form $\{1 \otimes \lambda_i\}$. The λ_i's are not uniquely determined, only $\operatorname{mod} pX$ ($p = \operatorname{char} k$), so we have to make a choice which we do. We then set $L_1 = \sum \mathbb{Q}\lambda_i \cap L$. Then $k \otimes L_1$ contains $\mathfrak{t}_1$ and on the other hand does not have a larger dimension, both by our construction. Thus the spaces are equal, (d) implies (b), and we are done.

3.4 Corollary. *The intersection of any family of algebraic subalgebras of* $\mathfrak{t}$ *is algebraic.* (*By the equivalence of* (a) *and* (c) (*or* (a) *and* (b)).

3.5 *Remark.* T_1 above is not in general uniquely determined by $\mathfrak{t}_1$ if $\operatorname{char} k = p \neq 0$, for, by adding arbitrary elements of pL to a basis for L_1, we may change L_1, hence also T_1, without changing $\mathfrak{t}_1 = k \otimes L_1$.

3.6 Lemma. *Let* T, $\mathfrak{t}$, *etc. be as above and* $H \in \mathfrak{t}$.

(a) *There exists a unique smallest algebraic subalgebra* $\mathfrak{t}_1$ *of* $\mathfrak{t}$ *containing* H.

(b) *Let* $H = \sum_{i=1}^{s} c_i \otimes \lambda_i \in k \otimes L$. *Then the following conditions are equivalent.*

(1) s *is minimal.*

(2) $\{1 \otimes \lambda_i\}$ *is a basis of* $\mathfrak{t}_1$ (*see* (a)).

(3) $\{c_i\}$ *and* $\{1 \otimes \lambda_i\}$ *are both linearly independent over* k_0.

(c) *If* $\chi \in X$, *then* $\chi(H) = 0$ *if and only if* $\chi(\mathfrak{t}_1) = 0$. *If* $\sigma \in \operatorname{Aut}(T)$, *then* σ *fixes* H *if and only if it fixes every point of* $\mathfrak{t}_1$. *In both cases* $\mathfrak{t}_1$ *may be replaced by* $\mathfrak{t}_1(k_0)$.

Proof. (a) This follows from 3.4.

(b) Clearly $\mathfrak{t}_1 \subseteq \langle\{1 \otimes \lambda_i\}\rangle$. Thus $\min s = \dim \mathfrak{t}_1$ and the minimum occurs exactly when $\{1 \otimes \lambda_i\}$ is a basis of $\mathfrak{t}_1$. The equivalence of (1) and (3) is a standard fact from elementary linear algebra.

(c) Write H minimally as in (b). If $\chi(H) = 0$, then $\sum c_i\chi(1 \otimes \lambda_i) = 0$, whence every $\chi(1 \otimes \lambda_i) = 0$ by (b3), and $\chi(\mathfrak{t}_1) = 0$ by (b2). The reverse conclusion is clear. If σ is as in (c), then $\sigma H = H$ if and only if $((1 - \sigma)X)(H) = 0$ and similarly with $1 \otimes \lambda_i$ in place of H. Thus the second part of (c) follows from the first, and the third from 3.3.

3.7 Lemma. *Let G be reductive, T a maximal torus, H an element or subset of* $\mathfrak{t}$, *and Σ', W', W'' as in* 2.14 *with H in place of t. Then the conclusions* (a), (b), *and* (c) *modified accordingly hold.*

Proof. For each root α, let $x_\alpha\colon k \to U_\alpha$ be a parametrization. For $H \in \mathfrak{t}$, we have the equation (*) $x_\alpha(c)H = H - c\alpha(H)X_\alpha$ with X_α a suitable nonzero tangent vector to U_α (the image under dx_α of the standard tangent vector to k^*, in fact), got by differentiating $x_\alpha(c)\, tx_\alpha(c)^{-1} = x_\alpha(c(1 - \alpha(t)))t$ in G. It follows that the parts of G listed in (a) are all in $Z_G(H)$. Conversely, let $x = bn_w u$ (normal form of [12, 6.3]) be in $Z_G(H)$. We also have (**) $x_\alpha(c)X_\beta = \sum c_i c^i X_{\beta+i\alpha}$ for suitable c_i's ($i \geqslant 0$). Hence $uH = H + \sum c_\alpha X_\alpha$ ($c_\alpha \in k$, $\alpha > 0$, $w\alpha < 0$), so that $n_w uH = n_w H + V$ ($V \in \mathfrak{u}^-$). Since also $n_w uH = b^{-1}H = H + U_1$ ($U_1 \in \mathfrak{u}$), we get $U_1 = 0$ so that b fixes H, and $V = 0$ so that u fixes H, and finally $n_w H = H$ so that w also fixes H. Now if $u = \Pi\, x_\alpha(c_\alpha)$ ($\alpha > 0$), then since u fixes H, it follows from (*) and (**) that $\alpha(H) = 0$ for every α in the support of u, by induction on the height of α. Thus (a) holds when H is a single element, hence, by induction, also when H is a set of several elements. The proofs of (b) and (c) are substantially as in 2.14 and will be omitted.

3.8 Corollary. *Let G be reductive and H a semisimple element of* $\mathfrak{g}$. *Then there is a unique minimal* (*one contained in all others*) *algebraic Lie subalgebra* $\mathfrak{t}_1$ *of* $\mathfrak{g}$ *containing H. Further $Z_G(H) = Z_G(\mathfrak{t}_1)$.*

3.9 Definition. By the *rank* of H we shall mean the dimension of $\mathfrak{t}_1$.

Proof. We use the fact that (in any algebraic group) every such H is in the Lie algebra of some maximal torus. This is proved like the corresponding result in the group (cf. [8, Exp. 6, Theorem 5]). Let T be such a torus, and let $\mathfrak{t}_1$ be as in 3.6. Then $Z_G(H) = Z_G(\mathfrak{t}_1)$ by 3.6(c) and 3.7. Let $\mathfrak{a}$ be any minimal algebraic subalgebra of $\mathfrak{g}$ containing H. We must show that $\mathfrak{a} = \mathfrak{t}$. Let A be a subgroup of G corresponding to $\mathfrak{a}$. Then H is in the Lie algebra of some torus of A. By minimality, A itself must be a torus, hence contained in some maximal torus T' of G. Now T and T' are maximal tori of $Z_G(H)^0$, i.e., of $Z_G(\mathfrak{t}_1)^0$, hence are conjugate there: ${}^xT' = T$. Then ${}^x\mathfrak{a} \subseteq \mathfrak{t}$, so that ${}^x\mathfrak{a} \subseteq \mathfrak{t}_1$ by 3.6, whence $\mathfrak{a} \supseteq {}^{x^{-1}}\mathfrak{t}_1 = \mathfrak{t}_1$ and $\mathfrak{a} = \mathfrak{t}_1$ by minimality, as required.

3.10 *Remark.* It is not known to the author whether 3.8 is true without the assumptions on G and H, or, more generally, whether the intersection of two algebraic subalgebras is always an algebraic subalgebra (if char $k \neq 0$).

3.11 COROLLARY. *In* char 0, $Z_G(H)$ *in* 3.7 *is connected for every subset* H *of* $\mathfrak{t}$.

Proof. Assume $w \in W''$. By a theorem of Chevalley [12, 1.21], w is a product of reflections each in W''. Let w_α be any of them. Then $(1 - w_\alpha)H = 0$ so that $\chi(1 - w_\alpha)H = 0$ for every $\chi \in X$, i.e., $(\chi, \alpha^*)\, \alpha(H) = 0$ by the formula for a reflection. Set $\chi = \alpha$, $(\chi, \alpha^*) = 2$. Then $2\alpha(H) = 0$, $\alpha(H) = 0$. Thus $\alpha \in \Sigma'$, $w_\alpha \in W'$, $w \in W'$. Hence $W'' = W'$ and $Z_G(H)$ is connected by 3.7(c).

3.12 *Remark.* A different proof in case $k = \mathbb{C}$ is given in [8, Lemma 5]. The proof just given presents two obstructions in char $p \neq 0$. The first is the extension of Chevalley's theorem. This turns out to be all right (see 4.6 below) as long as p is not a torsion prime for G. The second, involved in the step from $(1 - w_\alpha)H = 0$ to $\alpha(H) = 0$, is not so serious since we need only the existence of some $\chi \in X$ such that $(\chi, \alpha^*) = 1$, which we always have in case each component of type C_r is simply connected, hence if G itself is so.

Turning now to the case char $k \neq 0$, we shall prove the following analogues of 2.27 and 2.28.

3.13 THEOREM. *Let G be a reductive group and p a prime equal to* char k. *Then the following are equivalent.*

(a) $p \nmid F(G)$ *(see §2); i.e., the universal covering of the semisimple component of G is separable.*

(b) $Z_G(H)$ *is connected for every* rank-1 *semisimple element* H *of* $\mathfrak{g}$ (*see* 3.9).

3.14 THEOREM. *Let* G *and* p *be as in* 3.13. *Then the following are equivalent.*

(a) p *is not a torsion prime for* G.

(b) $Z_G(H)$ *is connected for every* rank $\leqslant 2$ *semisimple element* H *of* $\mathfrak{g}$.

(c) $Z_G(H)$ *is connected for every semisimple element* H *of* $\mathfrak{g}$.

(d) $Z_G(H)$ *is connected for every commutative set of semisimple elements of* $\mathfrak{g}$.

3.15 *Remarks.* (a) 3.11 and 3.14 yield Theorem 0.2 of the introduction.

(b) Conditions such as 2.28(d) have no place here since every set as in (d) can be put in the Lie algebra of some torus. We can prove this by starting with a single element H, proving the analogue of 3.7 with $Z_{\mathfrak{g}}(H)$ in place of $Z_G(H)$, and then proceeding by induction.

The proof of 3.13 and 3.14 depend on another transfer lemma. Let G and p be as above and let G' be of the same type as G but over an algebraically closed field k' of char $\neq p$. If T' is a maximal torus of G' and L', X', etc. are defined accordingly, we require the existence of an isometry from L onto L' matching up X with X', Σ with Σ', and W with W'. We may construct G', for example, by starting with the direct product of a simply connected semisimple group G'' and a torus T''', both over k', with Σ''^* matched up with Σ^* (hence L'' with $L(\Sigma^*)$) and L''' with the orthogonal complement of $L(\Sigma^*)$ in L, and then dividing out an appropriate finite subgroup of the center (which may be partly infinitesimal (see [2, §17])).

3.16 LEMMA. *Let* ψ *be a fixed isomorphism of the additive group of* k_0 *onto the group of* p*-th roots of* 1 *of* k' *and* φ *its extension from* $\mathfrak{t}(k_0)$ *onto the group* $T'(p)$ *of* p*-th roots of* 1 *of* T' (*cf.* 3.1). *Then the conclusions of* 2.32 *with the obvious substitutions hold.*

Proof. Like that of 2.32.

Proof of Theorems 3.13 *and* 3.14. Let T be a maximal torus of G and G', T', φ as in 3.16 so that φ maps $\mathfrak{t}(k_0)$ onto $T'(p)$ isomorphically. Let H, $H' = \varphi(H)$ be a corresponding pair of elements. Let W', W'' be defined for H as in 3.7, and W''', W'''' accordingly for H' as in 2.14. Then $W' = W'''$ and $W'' = W''''$ by 3.16, so that $Z_G(H)$ and $Z_{G'}(H')$ are isomorphic over their identity components by 3.7 and 2.14, hence are both connected or both disconnected. Since every rank-1 semisimple element of $\mathfrak{g}$ is conjugate to an element of $\mathfrak{t}(k_0)$ and every order p element of G' to an element of $T'(p)$, it follows that the conditions 3.13(b) for G and 2.27(b) for G' are equivalent. But the last condition is equivalent to 2.27(a) (for G'), which in turn is equivalent to 3.13(a) since $F(G) \sim L/L(\Sigma^*) \sim F(G')$ and char $k = p$, char $k' \neq p$. Thus (a) and (b) of 3.13 are equivalent and that theorem is proved. In the last three parts of 3.14, H may be replaced by a subspace of some $\mathfrak{t}(k_0)$, of dimension $\leqslant 2$ in part (b), without changing $Z_G(H)$, by 3.6 and 3.8. Hence (c) and (d) are equivalent and 3.14 can be deduced from 2.28 just as 3.13 has been deduced from 2.27, with the aid of 3.16 and a little care. We see further that $\leqslant$ may be replaced by $=$ in 3.14(b) in case $p \nmid |F|$, as in 2.28(b).

4. The Abstract Essence

The reader may have observed that in §3 once past 3.7 the discussion was no longer concerned with $\mathfrak{g}$ per se, only with the action of W on $\mathfrak{t}$, and similarly in §2. We wish to extract the geometric essence of those discussions in the form of extensions of Chevalley's theorem mentioned in 3.11. Thus to start with we assume given only a lattice L, its dual X, a finite reflection group W acting on L and X compatibly, and any Abelian group A. We write ${}^AL$ for $A \otimes_{\mathbb{Z}} L$ and wish to study $Z_W(H)$ when H is an element or subgroup of ${}^AL$; in §2 we did this for $A = k^*$ or $\mathbb{R}/\mathbb{Z}$, in §3 for $A = k$. The root system Σ is not given *a priori* so that we are free to choose it so as to facilitate our study. First we define Σ^* (as in [12, 3.6]) to consist of the minimal elements of L in the various directions in which the reflections of W take place. For each α^* in Σ^* there then exists α in $\mathbb{Q} \otimes X$ such that $\alpha(\alpha^*) = 2$ and $w_{\alpha^*}\lambda = \lambda - \alpha(\lambda)\alpha^*$ for all λ in L, and these α's form Σ. Here every $\alpha(\lambda)$ is in $\mathbb{Z}$ since α^* is primitive in L, so that each α is in fact in X. It is easily verified that Σ^* and Σ are root systems, the integrality coming from the above equation with $\lambda = \beta^* \in \Sigma^*$, so that we are in the situation of §2 and §3. Our choice of Σ^* also yields:

4.1 Lemma. *If H is a subset of ${}^AL$ and α a root, then $\alpha(H) = 0$ if and only if $w_\alpha \in Z_W(H)$.*

Proof. The last condition, $(1 - w_\alpha)H = 0$, i.e., $\alpha(H)\alpha^* = 0$ by the formula for a reflection, is equivalent to $\alpha(H) = 0$ since α^* is primitive.

The results we have in mind may now be stated, with $L, X, \ldots, A$ as we have just introduced them. By 2.14 and 3.7, the analogue in W of a subgroup of G that is connected is a subgroup that is generated by reflections. Therefore, for each subgroup Y of W we write Y^0 for its largest reflection subgroup, generated by the reflections that it contains.

4.2 THEOREM. *Let H be an element of ${}^AL$. Assume that every finite subgroup of A is cycle, or, equivalently, that* tors $X(H)$ *is cyclic.*

(a) *$Z_W(H)/Z_W(H)^0$ is isomorphic to a subgroup of $F =$* tors $L/L(\Sigma^*)$, *and if A contains an element of order n, then every subgroup of F of order n is realizable.*

(b) *If $H^n \in Z$, then $y^n = 1$ for all $y \in Z_W(H)/Z_W(H)^0$.*

Here Z denotes "the center" $Z_{A_L}(W)$.

4.3 COROLLARY. *$Z_W(H)$ is a reflection group in* (a) *in case $F = 0$, i.e. (W, L) is "simply connected," in* (b) *in case n is prime to $|F|$.*

This is clear.

4.4 *Remarks.* In theorems such as this the only elements of A that come into play are those of $X(H)$ so that the assumptions made are effectively equivalent. The condition on A is that it is imbeddable in some k^* (in $\mathbb{R}/\mathbb{Z}$ if A is small enough), so that in view of 2.14 and the fact that the data $L, X, \ldots, k$ are realizable in some reductive algebraic group, the above results may be extracted from 2.16. Alternatively, the earlier proofs may be transferred to the present context.

4.5 THEOREM. *Let H be any subgroup of ${}^AL$. Then $Z_W(H)/Z_W(H)^0$ is nilpotent. Let X^0 be the annihilator of H in X and p a prime. If X/X^0 has no p-torsion or if (L, W) has none, then $Z_W(H)/Z_W(H)^0$ and $L(\Sigma^*)/L(\Sigma'^*)$ have none.*

Here $\Sigma' = Z_\Sigma(H)$ and the torsion primes for (L, W) are meant to be those of 2.5.

4.6 COROLLARY. *If* tors X/X^0 *is relatively prime to* tors (L, W) *(resp.*

to tors Σ), *then* $Z_W(H)$ *is a reflection group* (*resp.* $Z_W(H)^0$ *is simply connected in* W).

In view of 4.5 this is clear.

4.7 *Remarks.* If A itself, or equivalently $X(H)$ by 4.4, is free from the torsion of (L, W) (resp. of $\sum$) in 4.6, then X/X^0 will always be torsion free (and similarly in 4.5). In particular, if A is $\mathbb{Z}$ or $\mathbb{R}$, hence has no torsion at all, we get Chevalley's theorem itself, made more precise by the condition in brackets. Another case, related to 2.17, in which the same strong conclusions hold, is that in which A is assumed to be divisible in 4.6, p-divisible in 4.5.

Proof of 4.5. This may be deduced from 2.24 as 4.2 from 2.16 once it is observed that ${}^{A}L$ may be replaced by ${}^{C}L$ and H by the annihilator of X^0 in ${}^{C}L$.

Now given an element H of order p, we may define its p-rank as the rank of the elementary p-group X/X^0, or, equivalently, of $X(H)$, and similarly if H is a subgroup. The obvious analogues of 3.13 and 3.14 are then true. Their formulations and proofs will be left to the reader.

Finally a word about duality. Let A^* be the character group of A into some Abelian group, so that ${}^{A^*}X$ is that of ${}^{A}L$. Then if we are interested in stabilizers in W of sets of characters, for example, for subgroups of T in §2, we may apply the preceding results with the roles of L and X, of Σ^* and Σ, and of A and A^* interchanged.

References

1. A. Borel, Sous-groupes commutatifs et torsion des groupes de Lie compacts connexes, *Tôhoku Math. J.* **13** (1961), 216–240.
2. A. Borel, "Linear Algebraic Groups," Benjamin, New York, 1969.
3. A. Borel *et al.*, "Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics", 131, Part E, Springer, Berlin, 1970.
4. A. Borel and F. Hirzebruch, Characteristic classes and homogeneous spaces III, *Amer. J. Math.* **82** (1960), 491–504.
5. A. Borel and J. de Siebenthal, Les sous-groupes fermés de rang maximum des groupes de Lie clos, *Comm. Math. Helv.* **23** (1949), 200–221.
6. N. Bourbaki, "Groupes et Algèbres de Lie," Chapters 4–6, Hermann, Paris, 1968.
7. B. Kostant, Lie group representations on polynomial rings, *Amer. J. Math.* **85** (1963), 327–404.

8. Séminaire C. Chevalley: "Sur la Classification des Groupes de Lie Algébriques," 2 Vol., Inst. H. Poincaré, Paris, 1956–58.
9. J.-P. Serre, "Corps Locaux," Hermann, Paris, 1968.
10. J. de Siebenthal, Sur les sous-groupes fermés connexes des groupes de Lie clos, *Comm. Math. Helv.* **25** (1951), 210–256.
11. R. Steinberg, "Lectures on Chevalley Groups," Yale University Math. Dept., 1968.
12. R. Steinberg, Endomorphisms of linear algebraic groups, *Amer. Math. Soc. Mem.* No. 80 (1968).